Cyber Security Commission
Cyber Infrastructure and Commonwealth Network Protection Working Group
Inaugural Meeting (Draft Minutes)

August 20, 2014
Teleconference, 3:30 pm until 4:15 pm

Chair:

Paul Kurtz, Chief Strategy Officer, CyberPoint

Members Present:

JC Dodson, BAE Systems
Betsy Hight, RADM USN Ret and HP Cybersecurity Practice.

Volunteers/Advisors/Staff in Attendance:

Rear Admiral Bob Day, Cyber Commission Staff Lead
Josh Heslinga, Office of the Attorney General, Cyber Commission Counselor
Isaac Janak, Office of Public Safety and Homeland Security
Dr. Jennifer Lee (for Secretary Hazel)
Mike Watson, VITA CISO

Public Members Present:

Debbie Hardy, SRC Corporation.
Mark Ingalls, Dominion Power.

Minutes

15:30 Roll call and introductions conducted by Rear Admiral Bob Day.

15:40 Chair Paul Kurtz reviewed the Draft 4 phase Work Plan (attached) with members and asked for feedback. Betsy Hight sought clarification on how the Work Group would be able to access Commonwealth and other resources to obtain the information needed to conduct the Work Plan inventories, assessments, and gap analysis. Paul Kurtz indicated that this did need to be worked out and posed the question to COV representatives on the call; Isaac Janak and Mike Watson believed that they could be the needed conduit to obtain needed COV agency access as well as any partnership groups COV is engaged with (i.e. Cyber Security Partnership and Infraguard). Isaac Janak is developing a list of COV, private, and Federal entities that are sharing Cyber information and this may be useful to the Work Group. Paul Kurtz stated that private sector access would likely be more challenging but much information could likely be generated from online searches, personal contacts of Work Group members, and on-site visits.

16:05 JC Dodson commented on the need to have an inventory of current COV laws and regulation related to Cyber including those that are currently being proposed. Bob Day and Isaac Janak will work with COV entities to develop this since it will likely be needed by all Work Groups. Mark Ingalls commented that Federal requirements that potentially drive COV requirements may also be needed. The Work Group decided to leverage the collaboration area on Innovate VA as much as possible.

16:10 Chair Kurtz summarized discussion and established a work group goal to:

a. Comment on the proposed work plan no later than close of business Friday 22 August. Finalized work plan to be submitted to Bob Day on 25 August.
b. Set up monthly meetings. Isaac Janak to coordinate.
c. When conducting review of Work Plan Phase 1 A/B/C, indicate the areas which you would desire to work on.

16:15 Bob Day requested Public Comment, none provided. Chair Kurtz closed the meeting.

Minutes recorded by Rear Admiral Bob Day

Attachment: Draft Work Group Plan

Cyber Infrastructure and Commonwealth Networks Protection Working Group

DRAFT Work Plan

Mission and Scope: review the adequacy of the security of the Commonwealth government's networks and make recommendations for improvements; review the cyber security of privately owned and operated critical infrastructure and make recommendations for improvements

I. Phase 1. Data Gathering (90 days):

A. Inventory of what protection programs we have in place

1. State government driven
2. Regional/metropolitan driven
3. University driven
4. Private sector driven
5. Federal
6. Public-Private partnerships (e.g. Virginia Cyber Security Partnership)

Any programs identified should be broken down by key economic sectors they support (transportation, energy, etc), and to capture program details such as its budget, key POCs, etc. Any issues and/or challenges associated with the program's execution should be identified and understood.

We do need to discuss how we can gather this data most effectively.

B. Inventory of programs in "the pipeline" or proposed programs

1. State government driven
2. Regional/metropolitan program
3. University driven
4. Private sector driven
5. Federal

C. Peer review of other States programs vs what VA has in place or planned (CA, NY, Colorado, TX, MD…) Extract useful ideas and recommendations as appropriate. We need to be able to tell the leadership how we compare.

II. Phase 2. Recommendation Development (90 days):

A. A vision statement for what VA should become with re to cyber infrastructure protection

B. Development of a list of critical shortfalls requiring urgent attention

C. Development mid to long term recommendations

D. Budget breakdown

III. Phase 3. WG Coordination. Cross check our thoughts and findings with other working groups (30 days)

IV. Phase 4. Report Writing (45 days)